UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of: Information associated with the account described in Attachment A within the possession, custody, or control of Dropbox, Inc.	)	Case No. 2:18-MJ-1488

APPLICATION FOR WARRANT PURSUANT TO 18 U.S.C. § 2703

I, a federal law enforcement officer, request a warrant pursuant to Title 18, United States Code, Section 2703, and state under penalty of perjury that I have reason to believe that within the following data:

See Attachment A

There are now concealed or contained the items described below:

See Attachment B

The basis for the search is:

☑ Evidence of a crime;
☑ Contraband, fruits of crime, or other items illegally possessed;
☐ Property designed for use, intended for use, or used in committing a crime.

The search is related to a violation of:

Code section(s)	*Offense Description*
18 USC §§ 872, 875(d), 1030, 2261A	Extortion, Computer Fraud, Stalking

The application is based on these facts:

See attached Affidavit, which is incorporated herein by reference.

Applicant's signature
Joseph Bennett, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: _____

Judge's signature

City and State: _____

Honorable Rozella A. Oliver,
U.S. Magistrate Judge
Printed name and title

AUSA: Khaldoun Shobaki x0759

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the following account that is within the possession, custody, or control of Dropbox, Inc., a company that accepts service of legal process at 333 Brannan Street, San Francisco, California 94107, regardless of where such information is stored, held, or maintained:

	Identifier(s)
1.	Email: managment42@yahoo.com User ID: 272969684
2.	The account associated with the following Dropbox link: https://www.dropbox.com/s/7v71v6pm5njb4he/IMG9870.scr?dl=0

ATTACHMENT B

ITEMS TO BE SEIZED

A. SEARCH PROCEDURE

1. The warrant will be presented to personnel of Dropbox, Inc. ("Dropbox" or the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.10.a. below), law enforcement agents and/or individuals assisting law enforcement and acting at their direction (the "search team") will examine such content records pursuant to search procedures specifically designed to identify items to be seized under this warrant. The search shall extract and seize only the specific items to be seized under this warrant (see Section III below). The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

5. If the search team encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

6. The search team will complete its search of the content records as soon as is practicable but not to exceed 120 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the content records beyond this 120-day period without first obtaining an extension of time order from the Court.

7. Once the search team has completed its review of the content records and created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the search team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, the search team will not access the data from the sealed original production which fell outside the scope of the items to be seized absent further order of the Court.

8. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

9. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

B. INFORMATION TO BE DISCLOSED BY THE PROVIDER

10. To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each SUBJECT ACCOUNT listed in Attachment A:

a. All contents of all wire and electronic communications associated with the SUBJECT ACCOUNT, limited to that which occurred on or after December 9, 2013,[6] including:

i. All media and files of any kind stored by the SUBJECT ACCOUNT, including any media or files previously uploaded, downloaded, viewed, shared, received, or accessed, photos and videos uploaded by or in connection with the SUBJECT ACCOUNT, where such media and files include any file type or extension, such as movies, videos, compressed .zip or .rar files, or any other type of file;

ii. Any links, Uniform Resource Locators ("URLs"), or other messages sent or received to or from the SUBJECT ACCOUNT, whether to or from the PROVIDER or other persons;

[6] To the extent it is not reasonably feasible for the PROVIDER to restrict any categories of records based on this date restriction (for example, because a date filter is not available for such data), the PROVIDER shall disclose those records in its possession at the time the warrant is served upon it.

iii. All e-mails, communications, or messages of any kind associated with the SUBJECT ACCOUNT, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each e-mail or message, and any related documents or attachments.

iv. All records or other information stored by subscriber(s) of the SUBJECT ACCOUNT, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files, and including specifically any metadata such as EXIF data associated with any pictures, photos, or videos;

v. All other records of communications and messages of any kind made or received by the user, including all private or instant messages, and specifically including all attachments to any messages in their native formats (for example, if a .zip or .rar file was sent to another user, the .zip or .rar file shall be provided), history of communications of any kind, video calling history, and where such records exist, the identity of any other user or account with which a SUBJECT ACCOUNT was connected;

vi. All records pertaining to communications between the PROVIDER and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken;

vii. All stored passwords, including passwords stored in clear text and hash form, and for any hashed values that include a salt, the PROVIDER shall provide the salt value used to compute the stored password hash value, and any security questions and answers;

viii. All search history, including searches made within Dropbox, web history, PROVIDER Web & App Activity or "History Events" by the user of the SUBJECT ACCOUNT, including web clicks;

ix. All web browsing activities that are identifiable with the SUBJECT ACCOUNT or with cookies used to access the SUBJECT ACCOUNT; and

x. All records (including content records) pertaining to any service associated with the SUBJECT ACCOUNT.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, e-mail addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, and including any changes

made to any subscriber information or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the following accounts:

(I) each SUBJECT ACCOUNT;

(II) any other account associated with the cookie(s) or machine cookies associated with a SUBJECT ACCOUNT;

(III) any other account associated with a SUBJECT ACCOUNT, including by means of sharing a common secondary, recovery, or alternate email address listed in subscriber records for the SUBJECT ACCOUNT or by means of sharing a common phone number or SMS number listed in subscriber records for the SUBJECT ACCOUNT;

(IV) any other account accessed by a device with an identifier responsive to the device identifiers called for in sub-paragraph vi below.

ii. All user connection logs and transactional information of all activity relating to the SUBJECT ACCOUNT described above in Section II.10.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations.

iii. All IP logs, including all records of the IP addresses that logged into the account;

iv. any and all logs of user activity and user agent string, including: web requests or HTTP requests; any logs containing information such as the Requestor's IP address, identity and user ID, date and timestamp, request URI or URL, HTTP protocol version, referrer, and other user agent string information; login tracker logs; account management logs; and any other information concerning web sites navigated to, other email or social media accounts accessed, or analytics related to the SUBJECT ACCOUNT;

v. Any and all cookies used by any computer or web browser associated with the SUBJECT ACCOUNT, including the IP addresses dates and times associated with the recognition of any such cookie;

vi. Any information identifying the device or devices used to access any SUBJECT ACCOUNT, including any Android ID, Advertising ID, unique application number, hardware model, operating system version, unique device identifiers, Global Unique Identifier or "GUID," serial number, mobile network information, phone number, device serial number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), International Mobile Equipment Identities ("IMEI"), or Apple advertiser ID or ID for advertisers ("IDFA"), and any other information regarding the types of devices used to

access each SUBJECT ACCOUNT or other device-specific information; and

vii. Any information showing the location of the user of a SUBJECT ACCOUNT, including while sending or receiving a message using a SUBJECT ACCOUNT or accessing or logged into a SUBJECT ACCOUNT.

C. INFORMATION TO BE SEIZED BY THE GOVERNMENT

11. For each SUBJECT ACCOUNT listed in Attachment A, the search team may seize:

a. All information described above in Section II.10.a. that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 872 (Extortion by Officers or Employees of the United States), 875(d) (Extortion via Interstate Transmission), 1030 (Computer Fraud), and 2261A (Stalking), namely:

i. Information relating to who created, accessed, or used the SUBJECT ACCOUNT, including records about their identities and whereabouts;

ii. Evidence indicating how and when the SUBJECT ACCOUNT was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the account owner;

iii. Information relating to the extortion, blackmail, or use of threats, including all photographs of persons other than Richard Gregory Bauer ("Bauer");

iv. Information relating to the LuminosityLink RAT malware or any other malware;

v. Information relating to computer programs or software that can be used to obtain or secure unauthorized access to a computer or computer network, including the actual use, development, or operation of such programs or software;

vi. Information relating to the results or effects of any unauthorized computer access, including deleting or overwriting files, exfiltrating or transferring data, evading detection, warnings or messages to victims conveyed by means of such access, or other damage, theft, or loss resulting from such access;

vii. Information relating to any files, information, folders, or other data taken from the computers, networks, emails, or any other information owned or maintained by any person other than Bauer;

viii. The identity and location of any users of the SUBJECT ACCOUNT or persons with whom they are in communication or communicating about; and

ix. All records and information described above in Section II.10.b.

D. PROVIDER PROCEDURES

12. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

Special Agent Joseph Bennett
4800 Oak Grove Drive | MS 180-205
Pasadena, CA 91109-8099
Phone: 818-354-9768

joseph.w.bennett@nasa.gov

IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

x

AFFIDAVIT

I, Joseph Bennett, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the National Aeronautics and Space Administration ("NASA"), Office of the Inspector General ("OIG") and have been so employed since March 2016. Prior to my current position with NASA OIG, I was employed by the United States Postal Inspection Service ("USPIS") as a United States Postal Inspector since September 2005. During my career, I have received specialized training in the investigation of computer crimes, combating the distribution of child pornography, and the performance of digital forensics. I am currently assigned to the Computer Crimes Division ("CCD") of NASA OIG, located at the Jet Propulsion Laboratory ("JPL") in Pasadena, California. I currently investigate computer and high-technology crimes, including computer intrusions, denial of service attacks and other types of malicious computer activity. During my career as a Special Agent, I have participated in numerous computer crime investigations. In addition, I have received both formal and informal training from FLETC Academy and other institutions regarding computer-related investigations and computer technology.

2. I make this affidavit in support of an application for a warrant for information associated with the following accounts (collectively, the "SUBJECT ACCOUNTS") that is stored at premises controlled by Dropbox, Inc. (the "PROVIDER"), a

provider of electronic communication and remote computing services, headquartered at 333 Brannan Street, San Francisco, California 94107[1]:

	Identifier(s)	**Name**
1.	Email: managment42@yahoo.com User ID: 272969684	SUBJECT ACCOUNT
2.	The account associated with the following Dropbox link: https://www.dropbox.com/s/7v71v6pm5njb4he/IMG9870.scr?dl=0	SUBJECT LINK ACCOUNT

3. The information to be searched is described in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A) and 2703(d)[2] to require the PROVIDER

[1] Because this Court has jurisdiction over the offense(s) being investigated, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

[2] The government is seeking non-content records pursuant to 18 U.S.C. § 2703(d). To obtain the basic subscriber information, which does not contain content, the government needs only a subpoena. See 18 U.S.C. § 2703(c)(1), (c)(2). To obtain additional records and other information--but not content--pertaining to subscribers of an electronic communications service or remote computing service, the government must comply with the dictates of section 2703(c)(1)(B), which requires the government to supply specific

to disclose to the government copies of the information (including the content of communications) described in Section II of Attachment B. Upon receipt of the information described in Section II of Attachment B, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachment B. Attachments A and B are incorporated herein by reference.

4. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with the SUBJECT ACCOUNTS constitutes evidence, contraband, fruits, or instrumentalities of criminal violations of 18 U.S.C. §§ 872 (Extortion by Officers or Employees of the United States), 875(d) (Extortion via Interstate Transmission), 1030 (Computer Fraud), and 2261A (Stalking).

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all

---

and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation in order to obtain an order pursuant to 18 U.S.C. § 2703(d). The requested warrant calls for both records containing content (see Attachment B paragraph II.10.a.) as well as subscriber records and other records and information that do not contain content (see Attachment B paragraph II.10.b.).

conversations and statements described in this affidavit are related in substance and in part only.

II. SUMMARY OF PROBABLE CAUSE

6. NASA OIG is currently investigating an extortion incident involving a NASA contract employee, Richard Gregory Bauer ("Bauer"). As set forth below, Bauer used his personal Facebook account to link his Facebook friends to malware stored in the SUBJECT ACCOUNTS.

III. STATEMENT OF PROBABLE CAUSE

A. Initial Investigation and Identification of BAUER

7. Between January 9 and 11, 2018, I conducted an initial investigation into an incident involving extortion of victim S.V., a contract employee at NASA Armstrong Flight Research Center ("NASA AFRC"). During that investigation, I learned the following:

a. S.V. reported receiving e-mails on her personal Google account claiming that explicit images of her would be revealed to NASA unless she complied with the sender's demands. She was also e-mailed additional sexually explicit photographs of herself.

b. The sender of the threatening messages used the Google account smit.steve432@gmail.com to send the threats to S.V.[3]

[3] On January 25, 2018, in Case No. 18-MJ-0184, the Honorable Steve Kim, U.S. Magistrate Judge for the Central District of California, issued a search warrant for smit.steve432@gmail.com. My review of the e-mail records for that account revealed numerous additional victims of extortion attempts similar to that made against S.V.

c. S.V. provided me with copies of the threatening communications. I, posing as S.V., then exchanged messages with smit.steve432@gmail.com, and received threatening e-mails intended for S.V. demanding sexually explicit photographs.

d. Records obtained from Google showed that the source Internet Protocol ("IP") address for the extortionate e-mails was 130.134.138.214 (the "NASA IP"), an IP address that I recognized as one associated with NASA.

e. I contacted the NASA AFRC Cyber Security Team and learned that the NASA IP was assigned to Bauer's NASA-issued laptop. I also learned that both Bauer and S.V. worked for the same contractor at NASA AFRC.

f. On January 11, 2018, I went to NASA AFRC to interview Bauer. With assistance from other law enforcement agents, I escorted Bauer from his workstation for the interview.

g. During the interview, Bauer told me the following, among other things:

i. He understood the term "extortion" and knew it to mean "blackmail";

ii. He admitted sending the e-mails containing explicit image demands to S.V.;

iii. He admitted that he sent similar e-mails to other victims requesting explicit images; and

iv. He had several other personal e-mail accounts, including but not limited to managment42@yahoo.com.[4]

[4] Note, "managment42" is not a typographical error—it is the correct spelling of the e-mail address used by Bauer.

8. During the interview, Bauer also provided written consent to search his personal laptop computer ("Bauer's Laptop"). Pursuant to that consent, I seized Bauer's Laptop for analysis.

B. Victim M.N.

9. On or about January 25, 2018, I was contacted by Detective William Fitzgerald of the Jacksonville-Florida Sheriff's Office. Fitzgerald told me that he was investigating e-mail extortion of victim M.N., and that most of the e-mails received by M.N. were associated with the NASA IP address. Fitzgerald provided me with the contact information for M.N.

10. On February 2, 2018, I contacted M.N. and conducted a telephonic interview. During that interview, among other things, M.N. told me:

a. On August 21, 2016, M.N. received a Facebook message from richard.bauer.9803 ("Bauer's Facebook Account"), asking if M.N. was willing to help him with a human studies course where his instructor wanted to interview people with some random questions. The questions Bauer asked included the following:

i. What was your major in college?

ii. Why did you pick that one?

iii. What was the first car you owned?

iv. Was it a gift or did you buy it out right?

v. Looking back, would you go to another university?

vi. What was the first concert you attended, were they your favorite band at the time?

b. M.N. perceived Bauer's questions to be innocent until she mentioned them to her boyfriend. M.N.'s boyfriend explained to her that the questions appeared to be security questions used to verify online user accounts.

c. M.N. received anonymous e-mails from the account garret.gman321@gmail.com on January 5, 2018, telling her that she must provide sexually explicit images of herself or else other sexually explicit images of her would be shared with others.

d. M.N. recalled that a friend, J.J., said that she received a request from Bauer's Facebook Account asking her to help test a new web application that Bauer claimed he had been developing. M.N. provided me with contact information for J.J.

e. M.N. provided me with copies of the messages discussed above.

C. Victim J.J.

11. On or about February 13, 2018, J.J. agreed to participate in a telephone interview. During that interview, among other things, J.J. told me the following:

a. On April 21, 2017, J.J. received a message from Bauer's Facebook Account, asking if J.J. was willing to help him by testing a new application that allowed him to take over her computer. J.J. provided a copy of the exchange with Bauer's Facebook Account, excerpted below:

BAUER:
Hey [J.J.] I have a favor to ask when you get a chance
J.J.:
hey whats yp; whats up?
BAUER:
Im developing an app and I was looking for people to try it out and see if it works ok
J.J.:
okay!
BAUER:
A computer app
J.J.:
do i download on the computer? That's probably a dumb question
BAUER:
Lol if you could yes please; NewAppTakeThree.jar [**attached a file named NewAppTakeThree.jar**];ive made some revisions to it, thus the name;let me know if you dont have the proper java installed and I can give you the link
J.J.:
okay! ill do it this weekend. Im actually packing for my trip home! i just logged on to print my reservation
BAUER:
oooooooo sorry! lol I thought you were free this weekend; you going to bama?

b. J.J.'s boyfriend told J.J. not to execute the program at the time and told her that she should not allow anyone to have access to her computer. J.J. never executed the program.

12. On February 16, 2018, NASA OIG Technical Investigator Behshad Sedighi ("Sedighi") and I met with J.J. and downloaded the "NewAppTakeThree.jar" file that was part of the Facebook conversation between J.J. and Bauer.

D. Facebook Search Warrant – Dropbox Victims

13. On April 10, 2018, in Case No. 18-MJ-0849, the Honorable Alexander F. MacKinnon, U.S. Magistrate Judge for the Central District of California, issued a search warrant for

Bauer's Facebook Account. On May 5, 2018, in response to the warrant, I received a copy of Bauer's Facebook Account from Facebook.

14. I have conducted a preliminary review of Bauer's Facebook Account. During my review, I found similar Facebook message exchanges between Bauer's Facebook Account and several of his Facebook friends attempting to cause them to download software under a variety of pretenses. In each of those conversations, Bauer asked his Facebook friends to download a file (believed to contain malware) from the SUBJECT ACCOUNT. Examples of those Facebook messages are excerpted below.

a. Facebook message thread that occurred on December 19, 2016 through February 9, 2017 between V.V. and Bauer's Facebook Account:

December 19, 2016

BAUER:
Would you be able to try out the app, well pseudo try out, the app and see if it works?
V.V.:
sure… lmk [let me know] what I have to do
BAUER:
so you should just be able to dl [download] that from dropbox and the app should open up with the screen saver picture . . . [**link to SUBJECT LINK ACCOUNT**]) . . . its basically a new/better way to view jpg but with higher quality

February 9, 2017

BAUER:
hey [V.V.] i have been working alot on the app and i was wondering if you could try it again for me if you have a min …its java based so you can just download it from this . . .[**attached a file named NewAppTakeTwo.jar**])

b. Facebook message thread that occurred on December 20, 2016 through March 21, 2017 between S.P. and Bauer's Facebook Account:

December 20, 2016

BAUER:
im doing some app development and I was wondering if you could test to see if it worked for me…basically its a way to save pictures in a new format for better quality than a .jpg . . . you might need to open it up manually since i havent been able to get windows to recognize me as a publisher . . . [**attached a file named "new app.zip"**]
S.P.:
Sure . . . It's not even letting me open/finish downloading the file
BAUER:
well let me try one thing… can you download it from my db [Dropbox]? [**link to SUBJECT LINK ACCOUNT**]
S.P.:
Same problem

January 7, 2017

BAUER:
hey [S.P.] when you get a free minute i wanted to take another crack at trying to give you my app to try again . . . [**attached a file named "NewPicAppWindows.jar"**]

c. From excerpted Facebook message thread that occurred on December 17, 2016 through March 21, 2017 between R.M. and BAUER'S Facebook Account:

December 17, 2016

BAUER:
… while i have someone i know would you mind testing the software for me? its a new picure viewer [**link to SUBJECT LINK ACCOUNT**]
R.M.:
it's not opening…

January 27, 2017

BAUER:
here is the updated version [**attached a file named "NewAppTakeTwo.jar"**]

E. Bauer Used and Distributed Luminosity Malware

15. As discussed above, on January 11, 2018, with written consent from Bauer, I seized Bauer's Laptop for analysis.

16. Sedighi conducted a forensic analysis of Bauer's Laptop, and informed me of, among other things, the following:

a. Sedighi discovered a "Luminosity" folder on the desktop of Bauer's Laptop. Based on research and analysis, this file folder is related to remote access trojan ("RAT")[5] software known as LuminosityLink.

b. Within the Luminosity folder, Sedighi discovered a file named "NewAppTakeThree.exe," a very similar name to file "NewAppTakeThree.jar," recovered from victim J.J. Based on my training and experience, I know that the ".jar," file extension signifies that the file received by J.J. was compressed for ease of delivery over Facebook.

c. Within the Luminosity folder, Sedighi discovered an executable file named "NewPicApp.exe." As discussed below, a similarly named "NewPicApp.jar" file was sent to victim J.H. using Facebook from a user identifying himself as Bauer.

d. Also within the Luminosity folder, Sedighi discovered text files containing e-mail addresses and other logins and passwords that appeared to have been generated by successfully installed LuminosityLink RAT malware.

---

[5] Based on my training and experience, I know that a RAT is a piece of malware (computer software) that allows unauthorized access to a victim's computer, and can allow a remote user (here, Bauer) to capture keystrokes, usernames, and passwords, in addition to copying files and surreptitiously activating webcams or other computer accessories.

17. On or about February 23, 2018, I compiled a list of e-mail addresses from the password files found on Bauer's Laptop and sent e-mails to each account, informing them that they were potential victims of a crime, and asking them to contact the me at their earliest convenience.

a. Victim J.H.

18. On or about February 26, 2018, J.H. responded to my e-mail and agreed to participate in a telephonic interview. During that interview, among other things, J.H. told me the following:

a. On January 6, 2017, J.H. received a Facebook message from Bauer's Facebook Account, asking if J.H. was willing to help him by testing a new application that "makes a jpg file into a newer one with better resolution." J.H. provided a copy of the Facebook messages with Bauer, excerpted below:

BAUER:
im developing an app that's used for either a pc or mac computer and i was wondering if you could see if it starts on your computer
J.H.:
(agrees)
BAUER:
[**attached a file named "NewPicApp.jar"**]
BAUER:
its an app that makes a jpg file into a newer one with better resolution.
BAUER:
[walked J.H. through Java install]
J.H.:
[eventually got Java installed]
BAUER:
it looked like it worked for a minute, I have a part of the app that tells me how many are currently using it

b. J.H. remembered executing the program but it did not appear to do anything. J.H. said that she still had the computer, but that it crashed sometime after this incident and the hard drive was replaced.

c. On August 24, 2017, J.H. received a Facebook message from "John Smith" that included a nude image of J.H. with the following messages:

i. "is this the [J.] that lives in woodland?"

ii. "you should read the email i sent you"

iii. "if you done want nude pictures on you on the internet respond back"

d. After receiving the Facebook message above, J.H. received an anonymous e-mail from Google account ss5705156@gmail.com threatening to distribute sexually explicit photographs of J.H. if she did not send new sexually explicit images.

e. J.H. provided me with copies of the threatening communications.

f. From records obtained from Google, I learned that one of the IP address associated to ss5705156@gmail.com is also associated with Bauer's residential Internet service.

19. On March 7, 2018, Sedighi and I met with J.H. to download the "NewPicApp.jar" application from her Facebook account. We also examined J.H.'s computer and found no existing malware. J.H. explained that her computer crashed in March 2017, and that she sent it to the manufacturer for repair. She was told that a new hard drive was installed.

F. Further Investigation re the PROVIDER

20. In connection with this investigation, I have identified numerous e-mail addresses associated with both Bauer and with extortion threats received by victims. I inquired with the PROVIDER about accounts linked with those addresses, and the PROVIDER identified accounts associated with two of those e-mail addresses: (a) the SUBJECT ACCOUNT, and (b) steve_smith12327@yahoo.com.

a. On April 9, 2018, in Case No. 18-MJ-0387, the Honorable Alexander F. MacKinnon, U.S. Magistrate Judge for the Central District of California, authorized a search warrant for an account held by the PROVIDER and linked to the second of those two addresses, steve_smith12327@yahoo.com.

b. The PROVIDER provided me with information showing that the IP addresses linked to the steve_smith12327@yahoo.com account included the NASA IP, and IP addresses associated with Bauer's current residence.

c. During my review of the materials provided in response to the search warrant on the PROVIDER account linked to steve_smith12327@yahoo.com, I located numerous images that were sent in extortionate e-mails, but I did not located any files connected to the LuminosityLink RAT malware.

21. Records produced by the PROVIDER about the SUBJECT ACCOUNT revealed the following:

a. The name used for the account is "Rich Bauer."

b. The e-mail address associated with the account was managment42@yahoo.com (the e-mail address identified by Bauer as his personal e-mail address during his interview).

c. User ID was 272969684.

d. Account created on March 2, 2014.

e. IP addresses linked to the account include the NASA IP, and IP addresses associated with Bauer's current and prior residences.

22. On or about May 24, 2018, I contacted the PROVIDER and asked if the PROVIDER could identify the SUBJECT LINK ACCOUNT based on the download link sent to numerous people from the Bauer Facebook Account, as discussed above and demonstrated in the Facebook message excerpts. The PROVIDER informed me that, in response to a search warrant, the PROVIDER would provide information for the account connected to a download link like that for the SUBJECT LINK ACCOUNT.

23. Based on the foregoing, and on my training and experience, I believe that:

a. There is probable cause to believe that Bauer used the LuminosityLink RAT malware to compromise victim computers and collect information from those computers, including photographs and other personal information, logins, and passwords.

b. There is probable cause to believe that Bauer used Bauer's Facebook Account to send some victims / Facebook friends a link to the SUBJECT LINK ACCOUNT in order to infect their computers with the LuminosityLink RAT malware.

c. There is probable cause to believe that the SUBJECT ACCOUNT is the same as the SUBJECT LINK ACCOUNT for a number of reasons, including:

i. It is one of two identified accounts connected to Bauer;

ii. Bauer identified the account in his Facebook messages as his Dropbox (i.e., PROVIDER) account;

iii. The SUBJECT ACCOUNT is connected to Bauer's personal e-mail address; and

iv. The search warrant executed on the other account linked to Bauer revealed materials related to extortion, but no LuminosityLink RAT malware, suggesting that it may be stored on a different account (i.e., the SUBJECT ACCOUNT).

A. Preservation Letter Request to the PROVIDER

24. On or about January 24, 2018, I sent the PROVIDER a preservation letter requesting that information associated with the SUBJECT ACCOUNT be preserved for 90 days pursuant to 18 U.S.C. § 2703(f).

25. On or about January 24, 2018, I received confirmation from the PROVIDER that pursuant to the preservation letter, they will preserve the records regarding the SUBJECT ACCOUNT for 90 days.

26. On or about April 27, 2018, I sent the PROVIDER a second preservation letter requesting that information associated with the SUBJECT ACCOUNT be preserved for additional 90 days pursuant to 18 U.S.C. § 2703(f).

27. On or about April 30, 2018, I received confirmation from the PROVIDER that pursuant to the preservation letter, they will preserve the records regarding the SUBJECT ACCOUNT for the additional 90 days.

IV. BACKGROUND REGARDING DROPBOX

28. Dropbox is a file hosting service that offers cloud storage, file synchronization, and client software to access Dropbox services. Dropbox allows users to store files in the cloud or on each of their computers using the Dropbox desktop client, which Dropbox then synchronizes so that it appears to be the same folder (with the same contents) regardless of which computer is used to view it. Files placed into Dropbox are also accessible through a website and mobile phone applications. Dropbox is also available on different platforms, such as on Linux systems, Android, BlackBerry OS, Apple iOS and MacOS, Windows, and others.

29. Dropbox also creates URLs (Uniform Resource Locators, i.e., website addresses) for its users, which one can share via email or through social media or networking applications. Sharing files can be accomplished by putting a file into a user's account, then sending it quickly by using a link. The link can be shared by email, chat or text message communication. Additionally, files can be sent to a Dropbox via Google's Gmail.

30. Dropbox is similar to other file-sharing and file-synchronizing services like Google's Drive. According to its website as of March 2018, there is a free version and various versions that require a monthly payment. The differences

between the plans include the amount of storage space available, additional sharing controls, unlimited file recovery, remote wipe/deletion of files, and the level of support that is available for customer service.

31. A subscriber of Dropbox may store many types of files in their Dropbox account, including media, address books, instant messages, emails, contact or buddy lists, calendar data, pictures (other than ones attached to emails), notes, documents, and other files, on servers maintained and/or owned by Dropbox. In my training and experience, evidence of who was using an account may be found in such information.

32. I have also learned that a provider like Dropbox will often track the behavior and activities of persons using accounts at the PROVIDER by using cookies. As noted above, these cookies can often show whether more than one account was accessed by the same computer. Specifically, Dropbox's website states that is uses "technologies like cookies and pixel tags," to among other things: "Log you in to our services," "Remember preferences and settings," "Keep your account secure," and "Better understand how people are using our services." In other words, Dropbox uses cookies to determine if the user of the account is the person who is accessing it, because Dropbox will recognize the cookie stored on the user's device. Based on my training and experience, such information can be useful in identifying the particular person or persons using a SUBJECT ACCOUNT.

33. In my training and experience, I have learned that providers of online services like Dropbox allow subscribers to obtain accounts like the SUBJECT ACCOUNTS. Subscribers obtain an account by registering with the provider. During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail or social media account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Some providers also maintain a record of changes that are made to the information provided in subscriber records, such as to any other e-mail addresses or phone numbers supplied in subscriber records. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of an account.

34. Therefore, the computers of the PROVIDER are likely to contain stored electronic communications and information concerning subscribers and their use of the PROVIDER's services, such as account access information, e-mail or message transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the SUBJECT ACCOUNT.

35. In my training and experience, online file-sharing services like Dropbox typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail and social media providers often have records of the Internet Protocol ("IP") address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the SUBJECT ACCOUNTS.

36. In my training and experience, users of online file-sharing services like Dropbox will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers of online storage services typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute

evidence of the crimes under investigation because the information can be used to identify the user(s) of the SUBJECT ACCOUNTS.

37. I know from my training and experience that the complete contents of an account may be important to establishing the actual user who has dominion and control of that account at a given time. Accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with sufficient information to identify other users of the account. Therefore, the contents of a given account, including the e-mail addresses or account identifiers and messages sent to that account, often provides important evidence regarding the actual user's dominion and control of that account. For the purpose of searching for content demonstrating

the actual user(s) of the SUBJECT ACCOUNTS, I am requesting a warrant requiring the PROVIDER to turn over all information associated with the SUBJECT ACCOUNTS with the date restriction included in Attachment B for review by the search team.

38. Relatedly, the government must be allowed to determine whether other individuals had access to the SUBJECT ACCOUNT. If the government were constrained to review only a small subsection of an account, that small subsection might give the misleading impression that only a single user had access to the account.

39. I also know based on my training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as “lol” to express “laugh out loud”), or codewords (which require entire strings or series of conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of a message or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and parenthesis :) to convey a smile or agreement) to discuss matters. “Keyword searches” would not account for any of these possibilities, so actual review of the contents of an account by law enforcement personnel with information regarding the identified criminal activity, subject to the search procedures

set forth in Attachment B, is necessary to find all relevant evidence within the account.

40. Users of online file-sharing services are often required to include an e-mail account as well as a phone number in subscriber records. The e-mail account may be an e-mail account hosted at the same provider, or an account at a different provider. The e-mail account is referred to by a number of names, such as a secondary e-mail account, a recovery e-mail account, or an alternative e-mail account or communication channel. That e-mail account is often used when the identity of the user of the primary account (here, the SUBJECT ACCOUNT) needs to be verified, for example if a password is forgotten, so that the provider can confirm that the person trying to access the account is the authorized user of the account. Similarly, the telephone number used in subscriber records is often used to send a passcode via text (or "SMS") that must be presented when trying to gain access to an account, either in a similar scenario where a user forgot his or her password, or when users implement what is referred to as "two-factor authentication" (where the password is one factor, and the passcode sent via text message to a mobile device is a second). In either scenario, the user of a primary e-mail account (the SUBJECT ACCOUNT) and a secondary e-mail account or phone number listed in subscriber records are very often the same person, or at least are close and trusted and/or working in concert. That is because access to either the secondary e-mail

account or to the phone number listed in subscriber records can allow access to the primary account.

41. Providers also frequently obtain information about the types of devices that are used to access accounts like the SUBJECT ACCOUNTS. Those devices can be laptop or desktop computers, cellular phones, tablet computers, or other devices. Individual computers or devices are identified by a number of different means, some of which are assigned to a particular device by a manufacturer and connected to the "hardware" or the physical device, some are assigned by a cellular telephone carrier to a particular account using cellular data or voice services, and some are actually assigned by the provider to keep track of the devices using its services. Those device identifiers include Android IDs, Advertising IDs, unique application numbers, hardware models, operating system versions, unique device identifiers, Global Unique Identifiers or "GUIDs," serial numbers, mobile network information, phone numbers, device serial numbers, Media Access Control ("MAC") addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"). Apple, one of the primary suppliers of mobile devices used to access accounts like the SUBJECT ACCOUNTS, had previously used an identifier that was unique to the hardware of its devices,

such that details of a device's activity obtained from a particular application or "app" could be used to target advertisements for the user of that device. Apple replaced that hardware-based identifier with the Apple advertiser ID or IDFA that is still unique to a particular device, but which can be wiped and re-generated anew by a user if a user chooses to do so. Most users, however, do not know that the IDFA exists, and therefore are unaware that their device's activity can be correlated across different apps or services.

42. These device identifiers can then be used (a) to identify accounts accessed at other providers by that same device, and (b) to determine whether any physical devices found in the course of the investigation were the ones used to access the SUBJECT ACCOUNTS. The requested warrant therefore asks for the device identifiers, as well as the identity of any other account accessed by a device with the same identifier.

43. This application seeks a warrant to search all responsive records and information under the control of the PROVIDER, which is subject to the jurisdiction of this court, regardless of where the PROVIDER has chosen to store such information.

44. As set forth in Attachment B, I am requesting a warrant that permits the search team to keep the original production from the PROVIDER, under seal, until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

a. I make that request because I believe it might be impossible for a provider to authenticate information taken from the SUBJECT ACCOUNTS as its business record without the original production to examine. Even if the provider kept an original copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the provider to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the provider to examine a particular document found by the search team and confirm that it was a business record of the provider taken from the SUBJECT ACCOUNTS.

45. I also know from my training and experience that many accounts are purged as part of the ordinary course of business by providers. For example, if an account is not accessed within a specified time period, it -- and its contents -- may be deleted. As a consequence, there is a risk that the only record of the contents of an account might be the production that a provider makes to the government, for example, if a defendant is incarcerated and does not (perhaps cannot) access his or her account. Preserving evidence, therefore, would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

V. CONCLUSION

46. Based on the foregoing, I request that the Court issue the requested warrant.

Joseph Bennett, Special Agent
National Aeronautics and Space Administration,
Office of the Inspector General

Subscribed to and sworn before me
on June 8, 2018.

HONORABLE ROZELLA A. OLIVER
UNITED STATES MAGISTRATE JUDGE